ARIZONA **STATEWIDE** **INFORMATION** **SECURITY**	**ADOA** **POLICY**	State of Arizona

ADOA POLICY 8310: ACCOUNT MANAGEMENT

DOCUMENT NUMBER:	P8310
EFFECTIVE DATE:	JULY 1, 2015
REVISION:	1.1

1. AUTHORITY

To effectuate the mission and purposes of the Arizona Department of Administration (ADOA), the Agency shall establish a coordinated plan and program for information technology (IT) implemented and maintained through policies, standards and procedures (PSPs) as authorized by Arizona Revised Statutes (A.R.S.)§ 41-3504 and § 41-3507.

2. PURPOSE

The purpose of this policy is to establish the baseline controls for the administration of state information system accounts.

3. SCOPE

3.1   **Application to ADOA Budget Units (ADOA BUs)** - This policy shall apply to all ADOA BU s as defined in A.R.S. § 41-3501(1).

3.2   **Application to Systems** - This policy shall apply to all state information systems:

1. **(P)** Policy statements preceded by "(P)" are required for state information systems categorized as Protected.

2. **(P-PCI)**Policy statements preceded by "(P-PCI)" are required for state information systems with payment card industry data (e.g., cardholder data).

3. **(P-PHI)** Policy statements preceded by "(P-PHI)" are required for state information systems with protected healthcare information..

4. **(P-FTI)** Policy statements preceded by "(P-FTI)" are required for state information systems with federal taxpayer information.

3.3   Information owned or under the control of the United States Government shall comply with the Federal classification authority and Federal protection requirements.

4. EXCEPTIONS

4.1 PSPs may be expanded or exceptions may be taken by following the Statewide Policy Exception Procedure.

4.1.1 Existing IT Products and Services

a. ADOA BU subject matter experts (SMEs) should inquire with the vendor and the state or agency procurement office to ascertain if the contract provides for additional products or services to attain compliance with PSPs prior to submitting a request for an exception in accordance with the Statewide Policy Exception Procedure.

4.1.2 IT Products and Services Procurement

a. Prior to selecting and procuring information technology products and services, ADOA BU SMEs shall consider ADOA and Statewide IT PSPs when specifying, scoping, and evaluating solutions to meet current and planned requirements.

5. ROLES AND RESPONSIBILITIES

5.1 State Chief Information Officer (CIO) shall:

a. Be ultimately responsible for the correct and thorough completion of Statewide IT PSPs throughout all state ADOA BU s.

5.2 State Chief Information Security Officer (CISO) shall:

a. Advise the State CIO on the completeness and adequacy of all state ADOA BU activities and documentation provided to ensure compliance with statewide IT PSPs throughout all state ADOA BU s;

b. Review and approve or disapprove all state ADOA BU security and privacy PSPs and exceptions to existing PSPs; and

c. Identify and convey to the State CIO the risk to state information systems and data based on current implementation of security controls and mitigation options to improve security.

5.3 ADOA BU Director shall:

a. Be responsible for the correct and thorough completion of ADOA BU PSPs;

b. Ensure compliance with ADOA BU PSPs; and

    c. Promote efforts within the ADOA BU to establish and maintain effective use of state information systems and assets.

5.4 ADOA BU CIO shall:

    a. Work with the ADOA BU Director to ensure the correct and thorough completion of ADOA BU IT PSPs; and

    b. Ensure ADOA BU PSPs are periodically reviewed and updated to reflect changes in requirements.

5.5 ADOA BU ISO shall:

    a. Advise the ADOA BU CIO on the completeness and adequacy of the ADOA BU activities and documentation provided to ensure compliance with ADOA BU Information Technology PSPs;

    b. Ensure the development and implementation of adequate controls enforcing the ADOA BU PSPs;

    c. Request changes and/or exceptions to existing PSPs from the State CISO; and

    d. Ensure all personnel understand their responsibilities with respect to secure account management.

5.6 Supervisors of state employees and contractors shall:

    a. Ensure users are appropriately trained and educated on ADOA BU PSPs; and

    b. Monitor employee activities to ensure compliance.

5.7 System Users of state information systems shall:

    a. Become familiar with this policy and related PSPs; and

    b. Adhere to PSPs regarding account management and acceptable use of state information systems.

6. ADOA POLICY

The ADOA BU shall implement account management through the following activities:

6.1 (P) **Automated Account Management** - The ADOA BU shall employ automated mechanisms to support the management of information system accounts. [NIST 800-53 AC-2(1)] [IRS Pub 1075] [PCI DSS 7.1.4]

6.2 (P) **Develop Account Management Operational Procedures** - The ADOA BU shall develop daily operational security procedures that are consistent with requirements in this specification. [PCI DSS 12.2]

6.3 **Identify Account Types** - The ADOA BU shall identify the types of state information system accounts to support organizational missions/ADOA business functions (e.g., individual, guest, emergency access, developer, maintenance, administration). [NIST 800-53 AC-2a] [HIPAA 164.312 (a)(2)(iii) – Addressable] [PCI DSS 7.2.2]

    6.3.1 **Establish Group and Role-based Accounts** - The ADOA BU shall establish conditions for group and role membership. [NIST 800-53 AC-2c] [PCI DSS 7.1.2] [PCI DSS 7.2.2]

    6.3.2 **Account Specification** -The ADOA BU shall specify authorized users of the state information system, group and role membership, and access authorizations (i.e., privileges) and other attributes for each account. [NIST 800-53 AC-2d]

    6.3.3 (P) **Privileged Accounts** - The ADOA BU shall restrict privileged accounts (e.g., super user accounts) on the state information system to administrative roles. [NIST 800-53 AC-6(5)] [IRS Pub 1075]

    6.3.4 (P) **Separation of Duties** - The ADOA BU shall separate ADOA BU -defined duties; documents separation of duties of individuals; and defines state information system access authorizations to support separation of duties. [NIST 800-53 AC-5] [IRS Pub 1075]

6.4 **Assign Account Managers** - The ADOA BU shall assign account managers for state information system accounts. [NIST 800-53 AC-2b]

6.5 **Account Approval** - The ADOA BU shall require documented approvals by authorized ADOA BU staff for requests to create, modify, and enable state information system accounts. [NIST 800-53 AC-2e-f] [PCI DSS 7.1.3]

    6.5.1 (P) **Automated Audit Actions** - The ADOA BU shall ensure the state information system automatically audits account creation, modification, enabling, disabling, and removal actions and notifies, as required ADOA BU-defined personnel or roles. [NIST 800-53 AC-2(4)] [IRS Pub 1075]

6.6 **Account Monitoring** - The ADOA BU shall authorize, and monitor the use of state information system accounts. [NIST 800-53 AC-2g]

    6.6.1 (P) **Vendor Account Monitoring** - The ADOA BU shall enable accounts used by vendors for remote access only during the time period needed and monitors the vendor remote access accounts when in use. [PCI DSS 8.5.6]

6.7 **Account Removal** - The ADOA BU shall notify account managers when accounts are no longer required; users are terminated or transferred; and individual information system usage or need-to-know changes. [NIST 800-53 AC-2h] [PCI DSS 8.5.4]

6.7.1 (P) **Immediate Removal of Terminated Users** - The ADOA BU shall immediately revoke access for any terminated users. [PCI DSS 8.5.4]

6.7.2 (P) **Automatic Removal of Temporary Accounts** - The state information system automatically removes or disables temporary and emergency accounts after a ADOA BU-defined time. [NIST 800-53 AC-2(2)] [IRS Pub 1075]

6.7.3 (P) **Disable Inactive Accounts** - The ADOA BU shall ensure the state information system automatically disables inactive accounts after ADOA BU -defined time period. For state information systems containing cardholder data (CHD) the time period must be no more than 90 days. [NIST 800-53 AC-2(3)] [IRS Pub 1075] [PCI DSS 8.5.5]

6.8 **Access Authorization** - The ADOA BU shall authorize access to the state information system based on a valid access authorization; intended system usage; and other attriADOA BU tes as required by the organization or associated mission functions. [NIST 800-53 AC-2f,i] [HIPAA 164.308 (4)(ii)(B) – Addressable]

6.8.1 (P) **Default "Deny-All" Setting** - The ADOA BU shall ensure the state information system access control system is set to "Deny all" unless specifically allowed. [PCI DSS 7.2.3]

6.8.2 (P) **Restrict Direct Database Access** - The ADOA BU shall ensure the state information system authenticates all access to any database containing Confidential information and restricts direct access or queries to databases to database administrators. [PCI DSS 8.5.16]

6.9 **Accounts Rights Review** - The ADOA BU shall review accounts for compliance with account management requirements annually. [NIST 800-53 AC-2j] [HIPAA 164.308 (4)(ii)(C) – Addressable]

6.10 **Reissues Account Credentials** - The ADOA BU shall establish a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group. [NIST 800-53 AC-2k]

7. DEFINITIONS AND ABBREVIATIONS

7.1 Refer to the PSP Glossary of Terms located on the ADOA-ASET website.

8. REFERENCES

8.1 ADOA Policy Exception Procedure

8.2 NIST 800-53 Rev. 4, Recommended Security Controls for Federal Information Systems and Organizations, February 2013.

8.3 HIPAA Administrative Simplification Regulation, Security and Privacy, CFR 45 Part 164, February 2006

8.4 Payment Card Industry Data Security Standard (PCI DSS) v2.0, PCI Security Standards Council, October 2010.

8.5 IRS Publication 1075, Tax Information Security Guidelines for Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information, 2010.

9. ATTACHMENTS

None.

10. REVISION HISTORY

Date	Change	Revision	Signature
04/01/2014	Initial release within ASET	1.0	Aaron Sandeen, State CIO and ADOA Deputy Director
08/01/2014	ADOA Assistant Director's review; approved revisions added Initial release within ADOA	1.1	Brian C. McNeil, ADOA Director